REMARKS/ARGUMENTS:

The claims have been amended above to respond to the Examiner's objections, which are now rendered moot.

In the Office Action mailed 12/10/2008 the Examiner now rejects claims 2, 3, 5, 6, 8, 9, 20, 23, 33-37, 39, 40, 46, 52-58 and 60 under 35 USC 102(e) as being taught by Meffert et al. (newly cited), and rejects claims 7, 38 and 59 under 35 USC 103(a) as being unpatentable over Meffert et al. in view of Schoch et al. (newly cited). These rejections are respectfully disagreed with, and are traversed below.

The Examiner is using the DRM aspects of Meffert et al., in particular those portions concerned with enabling a trial play of an encrypted MP3 file.

The independent claims 20, 33, 46 and 60 have been amended above to even further clarify the claimed subject matter, and to even further distinguish these claims from Meffert et al. Support for the amendments may be found in the instant specification as filed at least at page 6, lines 8-21. Newly added claims 61-64 are supported as well at least at this location.

As now presented for examination claim 20 recites:

> A method comprising:
> a) storing a plurality of data assemblages in a hand portable device;
> **a1) automatically discriminating between at least one defined type of data assemblages that contain user personal data and other types of data assemblages that do not contain user personal data;**
> b) storing at least one data attribute **for each of a plurality of first data assemblages that contain the user personal data**, the data attribute indicative of a first display of a corresponding first data assemblage in the device;
> c) displaying for a first time in the hand portable device a first data assemblage of the plurality of first data assemblages without regard to a first security mechanism, and responsive to the displaying for the first time automatically changing the data attribute of the displayed one of the first data assemblage from a first type to a second type; and
> d) in response to changing the data attribute of step c), automatically restricting further display of the first data assemblage using the first security mechanism.

As now presented for examination claim 33 recites:

> A hand-portable device comprising:
> an input configured to receive a password;
> a memory configured to store data;
> a display configured to display the data; and
> a processor configured to **automatically discriminate between at least one defined type of data assemblages that contain user personal data and other types of data assemblages that do not contain user personal data,** said processor further configured to **detect that certain data corresponding to a data assemblage that contains user personal data** has been displayed for a first time at the display and automatically responsive to detecting that the certain data has been displayed for the first time to restrict subsequent display of the certain data using a first security mechanism involving the password, wherein the processor does not restrict the certain data being displayed for the first time using the password.

As now presented for examination claim 46 recites:

> A memory storing a computer program and readable by a processor for enabling a mobile telephone to perform actions directed to restricting access to a first data assemblage, the actions comprising:
> a) storing a plurality of data assemblages in a mobile telephone;
> a1) **automatically discriminating between at least one defined type of data assemblages that contain user personal data and other types of data assemblages that do not contain user personal data;**
> b) storing at least one data attribute **for each of a plurality of first data assemblages that contain the user personal data**, the data attribute indicative of a first display of a corresponding first data assemblage in the mobile telephone;
> c) displaying for a first time in the mobile telephone a first data assemblage of the plurality of first data assemblages without regard to a first security mechanism, and responsive to the displaying for the first time automatically changing the data attribute of the displayed one of the first data assemblage from a first type to a second type; and
> d) in response to changing the data attribute of step c), automatically restricting further display of the first data assemblage in the mobile telephone using the first security mechanism.

As now presented for examination claim 60 recites:

> A hand-portable device comprising:
> user input means for user input of a password;
> memory means for storing data;
> display means for displaying the data; and

> access control means configured to **automatically discriminate between at least one defined type of data assemblages that contain user personal data and other types of data assemblages that do not contain user personal data**, and to **detect that the data of a data assemblage that contains user personal data** has been displayed for a first time at the display means and automatically responsive to detecting that the data has been displayed for the first time to restrict subsequent display of the data of the data assemblage that contains user personal data using a first security mechanism involving the password, wherein the access control means does not restrict the data of the data assemblage that contains user personal data being displayed for the first time using the password.

Clearly, the subject matter that is now recited in each of the independent claims is not expressly disclosed or suggested by the teachings of Meffert et al. For example, paragraph [0037] Meffert et al. state only that:

> Objects of the present invention include the provision of providing an Internet-based PKI-based encryption system and method that sends data such as documents, email, music files, XML content, etc., (hereinafter "content") easily and securely, with the minimum possible user intervention. In accordance with an important aspect of the present invention, the system provides life-of-content security, i.e., the system controls use of the content even after it has been sent or conveyed, with a full menu of restrictions including, for example, "do-not-print-or-forward" and "self-destruct". Accordingly, even if a computer or device on which the content is stored were stolen or fell into the wrong hands for even a limited amount if [sic, of] time, the content that has been encrypted in accordance with the present invention remains secure and readable only by the intended recipient. In the following description a "recipient" is meant to include anything that receives content. Thus, a person as well as electronic devices and electronic processes are considered recipients with the context of the present invention.

The paragraph [0120], referred to by the Examiner several times, recites only:

> As stated, the encrypted content 5522 includes all of the audio frames necessary to play the MP3 file. This encrypted data also includes DRM data including trial and purchased play rights and public keys associated with differing levels of access, namely, "trial", "play" and "song". The "trial" level access permits the user is permitted to listen to the song/track once, or within a date/time window, and thereafter is precluded from listening without again obtaining the proper authorization. The "play" level access permits the user to play the song/track a predetermined number of times, e.g., five times. After the fifth play, the song/track remains encrypted until the user obtains the appropriate authorization by, for example, paying for such additional use. Finally, the "song" level access permits the user to buy the song/track whereby the user can have unlimited access to the song or track.

Clearly, the disclosure of Meffert et al. of encrypted data that also includes DRM data "including trial and purchased play rights and public keys associated with differing levels of access" does not anticipate or suggest, e.g., as in claim 20 "**automatically discriminating between at least one defined type of data assemblages that contain user personal data and other types of data assemblages that do not contain user personal data" and/or** "storing at least one data attribute **for each of a plurality of first data assemblages that contain the user personal data**, the data attribute indicative of a first display of a corresponding first data assemblage in the device", and/or "displaying for a first time in the hand portable device a first data assemblage of the plurality of first data assemblages without regard to a first security mechanism, and responsive to the displaying for the first time automatically changing the data attribute of the displayed one of the first data assemblage from a first type to a second type", and/or in response to changing the data attribute "automatically restricting further display of the first data assemblage using the first security mechanism".

All other claims depend from one of claims 20, 33, 46 or 60, and should be allowable at least for that reason alone, whether considered only in view of Meffert et al. or in view of Meffert et al. and Schoch et al. (the proposed combination of which is not admitted is suggested or appropriate). None are argued separately here though the Applicants reserve the right to do so without prejudice should it later become necessary. The newly added claims 61-64 are thus also clearly patentable over the references cited and applied by the Examiner.

The Applicants thank the Examiner for the additional search and examination, and respectfully request that claims 2, 3, 5-9, 20, 23, 33, 34, 36-40, 46 and 51-64 now be passed to issue. The undersigned attorney welcomes the opportunity to discuss the claims and references and resolve any matters that may remain via teleconference at the Examiner's discretion.

Respectfully submitted:

3/13/2009

Harry F. Smith
Reg. No.: 32,493

Date

Customer No.: 29683
HARRINGTON & SMITH, PC
4 Research Drive
Shelton, CT 06484-6212

Phone: (203) 925-9400, ext 15
Facsimile: (203) 944-0245
Email: hsmith@hspatent.com

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

3/13/2009
Date

Elaine F. Main
Name of Person Making Deposit